ZEROFOX INTELLIGENCE

Flash

Prominent Threat Collective Announces Disbandment

F-2025-09-16a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Threat Actor, Deep Web, Data Breach

September 16, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on September 16, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Prominent Threat Collective Announces Disbandment

| Key Findings

- On September 11, 2025, the prominent threat collective "Scattered Lapsus$ Hunters" announced on its public Telegram channel that it was ceasing operations.[1] The message also appeared on the homepage of breachforums[.]hn, with a link to the collective's Telegram page.
- In the post, Scattered Lapsus$ Hunters explained that it is intentionally disbanding now that its objectives have been fulfilled. The collective emphasized that this decision is not a defeat or reaction to law enforcement (LE) pressure but rather the planned conclusion of a campaign.
- Although Scattered Lapsus$ Hunters claims to have ceased operations, it is likely that its Indicators of Compromise (IOCs) remain relevant for detection and hunting and that credentials and malware associated with the threat collective are still active or may resurface in future incidents.

[1] hXXps://t[.]me/sctt3rd/1601

Details

On September 11, 2025, prominent threat collective Scattered Lapsus$ Hunters announced on its public Telegram channel that it was ceasing operations.[2] The message also appeared on the homepage of breachforums[.]hn, with a link to the collective's Telegram page. Notably, as of writing, ZeroFox has observed that the main private Telegram channel associated with Scattered Lapsus$ Hunters is no longer available, providing further indication of the collective's cessation.

- On August 8, 2025, a new account named "scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS" surfaced on Telegram. The channel was launched by individuals claiming to be part of the prominent cybercrime collectives "Scattered Spider", "Lapsus$", and "ShinyHunters".
- On August 11, 2025, the scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS channel was banned from Telegram; however, the group quickly migrated to a new backup channel. In its brief four-day lifespan, posts on the scattered lapsu$ hunters - The Com HQ SCATTERED SP1D3R HUNTERS channel resembled the types of activity displayed within the Telegram channels operated by Scattered Spider, ShinyHunters, and Lapsus$.
- ZeroFox has observed several iterations of Telegram channels claiming to be associated with Scattered Lapsus$ Hunters. However, we cannot verify which accounts are legitimate.
- See ZeroFox's Flash report from August 13, 2025, "Threat Collectives Seemingly Announce Collaboration."[3]

[2] *Ibid.*
[3] https://www.zerofox.com/intelligence/flash-report-threat-collectives-seemingly-announce-collaboration/

Dear World,

We apologise for our silence and the ambiguities of our message, whose sole destinataries did not understand the profound meaning.

These 72 hours spent in silence have been important for us to speak with our families, our relatives, and to confirm the efficiency of our contingency plans and our intents.

These 72 hours had hoped for a long time.

As you know, the last weeks have been hectic. Whilst we were diverting you, the FBI, Mandiant, and a few others by paralyzing Jaguar factories, (superficially) hacking Google 4 times, blowing up Salesforce and CrowdStrike defences, the final parts of our contingency plans were being activated.

You might or might not have realized, but our behaviour evolved recently. When we entered into Google systems, we decided not to pursue over a certain point. In between others, we willingly left them in wonder of whether Google's Workspace, Person Finder, GMAIL including legacy branches got dominated.

This has been happening more and more, as we decided to progressively abandon some of our tools (Hello, Tutanota) and our correspondents to their own faith.

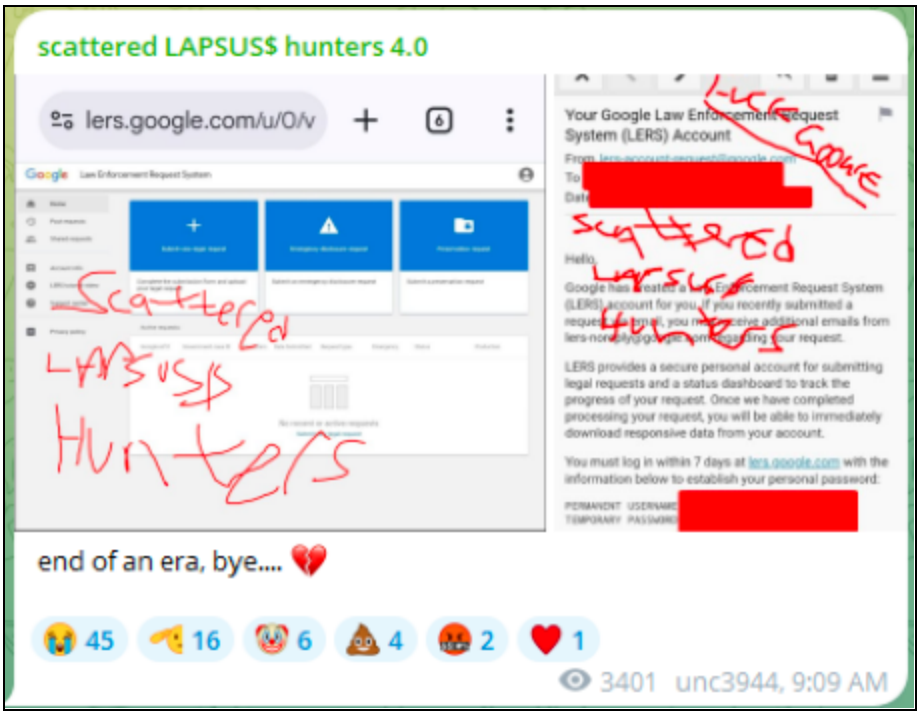
Will Kering, Air France, American Airlines, British Airlines, and among many other critical infrastructure face THE CONSEQUENCES OF THEIR PUBLIC OR SECRET databreaches? I'd wonder too if I was them, as they know some have yet to receive any demand for ransom - or anything else.

Message on BreachForums

Source: hXXps://breachforums[.]hn/

In the post, Scattered Lapsus$ Hunters explained that it is intentionally disbanding now that its objectives have been fulfilled. The collective emphasized that this decision is not a defeat or reaction to LE pressure but rather the planned conclusion of a campaign. In the past few months, the collective has claimed to have conducted high-profile attacks—targeting companies such as Google, Jaguar, Salesforce, and CrowdStrike—to divert the attention of the Federal Bureau of Investigation (FBI) and U.S.-based cybersecurity firm Mandiant while it was finalizing internal "contingency plans." Although no details were provided in the post regarding the nature of the contingency plans, they likely refer to safely transferring acquired financial gains and shutting down operations to mitigate the risk of LE detection.

- Furthermore, Scattered Lapsus$ Hunters strongly implied that there would be future data leaks from attacks it has already conducted on victims that have not yet publicly disclosed breaches.



Post on Scattered Lapsus$ Hunters' official Telegram channel

Source: hXXps://t[.]me/sctt3rd

Since the announcement of the threat collective's collaboration, a multitude of cyberattacks have resulted in several prominent disclosed victims—each seemingly linked to Scattered Lapsus$ Hunters. Notably, the collective has been tied to the recent Google Law Enforcement Request System (LERS) and Salesforce breaches, among several others—some of which are likely reused or repackaged previously compromised datasets. While its claimed breaches are notable, ZeroFox cannot verify the authenticity or accuracy of the collective's claims at this time.

- On September 15, 2025, Google acknowledged that a threat actor had created a fraudulent account within its LERS. The company claimed that the fake account has since been disabled, no requests were ever submitted via that account, and no data was accessed.[4] While the actor remains unknown, on September 12, 2025, the Scattered Lapsus$ Hunters collective posted a screenshot of the LERS portal on its Telegram channel.

[4] hXXps://www.bleepingcomputer[.]com/news/security/google-confirms-fraudulent-account-created-in-law-enforcement-portal/

- In June 2025, a prominent breach of a Paris-based parent company of luxury fashion brands, wherein customers' personally identifiable information (PII) and spending records were reportedly stolen, was attributed to ShinyHunters.[5]
- In August 2025, a sophisticated supply chain breach targeting the Drift-Salesforce integration leveraged OAuth credentials to exfiltrate Salesforce instance data from multiple companies. The attack was reportedly linked to the Scattered Lapsus$ Hunters collective.[6]

Although Scattered Lapsus$ Hunters claims to have ceased operations, it is likely that its IOCs remain relevant for detection and hunting and that credentials or malware associated with the threat collective are still active or may resurface in future incidents. Victims who have been targeted in previous attacks—particularly those not yet publicly named or extorted—are very likely still vulnerable to data exposure or delayed leaks. Scattered Lapsus$ Hunters' notoriety and media exposure will likely increase the risk of operational or actor impersonation, especially from less sophisticated threat groups seeking to capitalize on the threat collective's operational success and reputation.

[5] hXXps://hackread[.]com/gucci-balenciaga-alexander-mcqueen-breach-shinyhunters
[6] hXXps://trust.salesloft[.]com/?uid=Drift%2FSalesforce+Security+Update

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multifactor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%